ABSTRACT

The invention uses a layer 2 Ethernet switching device to establish two new port types, 'trusted ports' and 'un-trusted ports'. Devices connected to trusted ports on the switch (such as centrally managed file, email, print, and web servers) are permitted by default to transmit to and receive data from any device attached to the switch, whether attached to a trusted or an un-trusted port. Devices connected to un-trusted ports (such as end-user laptops, workstations, mobile devices, and other systems at greater risk of virus and worm infection), are permitted only to establish connections to devices attached to the trusted ports on the switch. The premise of the invention is provide a simplified system and methods to safeguard the confidentially, availability, and integrity of network-based information assets by reducing the total number of computer systems that an unauthorized user or application (e.g., hacker, worm, or virus) can connect to and attempt to exploit vulnerabilities on.